The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff<br><br>v.<br><br>PAIGE A. THOMPSON,<br>Defendant. | NO. CR19-159 RSL<br><br>UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR A *BRADY* ORDER |

The government takes its *Brady* obligations seriously, as shown by this office's proactive efforts to obtain and produce materials held by other Department of Justice components as soon as we learned those materials existed. This discovery production is evidence that the government understands and is complying with its *Brady* obligations and that a *Brady* order is unnecessary. Even if the Court were inclined to issue an order reminding the government of its *Brady* obligations, the Court should give the Due Process Protection Act admonition that is now routinely given in this District, and which was adopted by the Western District of Washington after careful consultation with the Office of the United States Attorney and the Office of the Federal Public Defender, rather than the much-more-broadly-worded order proposed by the defense.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## I. FACTS

The Court is familiar with the underlying facts of this case; therefore, this response focuses on the facts relevant to Thompson's motion.

### A. Warnings, and Possible Warnings, to Capital One about Thompson's Activity

In March 2019 and April 2019, internal Capital One Financial Corporation cyber security systems produced automated alerts that, in retrospect, appear to have been triggered by Paige Thompson's hacking activity. Those alerts were two of the myriad alerts that Capital One cyber security systems regularly provide about possible malicious activity. In each the two instances that apparently were triggered by Thompson's activity, a Capital One employee analyzed the activity that had triggered the alert and concluded that the activity was benign rather than malicious.

On or about May 20, 2019, an unknown individual passed an Amazon employee a note regarding a security vulnerability at a specific Amazon Web Services (AWS) IP address. The vulnerability was described as "an open socks proxy" that "Can Hit IMS – Lots of Security Credentials." Amazon looked up the IP address, determined that it belonged to Capital One, and forwarded the note to Capital One. Capital One took the note seriously and investigated, but was unable to find the security vulnerability identified by the note. Because no vulnerability was evident, Capital One ultimately determined that the May 2019 note was a false alarm.

Several months later, in July 2019, Capital One received a responsible-disclosure email from a person other than Thompson with a link to several files on Thompson's GitHub page. One of those files was created on April 21, 2019 ("the April 21 File"). The April 21 File listed folders that were stored on Capital One's servers and included an example of the commands that pulled security credentials from the same IP address that had been identified in the May 2019 note. Only then did Capital One realize that its servers had been breached, and only then did Capital One consider a potential connection between the April 21 file and the May 2019 note. Even so, the May 2019 note



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

inaccurately described the security vulnerability Thompson exploited as an "open socks proxy," which was not the type of computer protocol Thompson had used to access Capital One's servers and steal data in March 2019. Although Capital One employees have speculated about whether Thompson was behind the note, that fact has not been established.

**B. Information about the May 2019 note was disclosed to Thompson's defense team by Capital One in July 2021.**

As the Court knows, Capital One provided material directly to the defense, both in response to subpoenas and to less formal requests. For example, on July 27, 2021, Capital One provided information about the May 2019 note, to the defense. Exhibit 1. Capital One also provided information about the March and April 2019 alerts to the defense.

In mid-January 2022, as the government was preparing for trial, Capital One provided the government with a copy of the materials that it had provided to the defense. In following up with Capital One about these materials, and preparing to interview potential Capital One trial witnesses, our office learned from Capital One that it also had provided documents to Main Justice, and had made a subsequent presentation to Main Justice, about the March and April 2019 alerts triggered in its systems by Thompson's activity and about the May 2019 note.

**C. Our office promptly produced the Main Justice materials to the defense as soon as we learned that those materials existed.**

Upon learning that Capital One materials had been provided to Main Justice, our office followed up with Main Justice to determine what materials it had received. Main Justice indicated that, in addition to Capital One's presentation, it had received approximately 600 pages from Capital One, and that it had conducted interviews of two Capital One employees (which had not been memorialized in memoranda or reports). This was the full scope of the materials that Main Justice gathered.

Our office promptly requested, and received, from Main Justice the documents, the presentation, and the notes of the two interviews. After removing duplicate pages that



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Capital One had already provided to the defense, on February 15, 2022, the government produced approximately 300 non-duplicative pages,[1] the PowerPoint slide deck from Capital One's presentation to Main Justice,[2] and the notes from the two witness interviews. The government did not withhold any materials on the basis of materiality or privilege (or on any other basis).

Our office also confirmed with Main Justice and with the Southern District of New York (which received the initial contact from Capital One after it discovered Thompson's breach in July 2019, but which transferred the referral to our office within 24-48 hours), that neither had received or gathered any materials, beyond those already produced by our office in discovery to the defense. Our office also confirmed with Capital One that it had not provided any documents or information to any other component of the Department of Justice, other than Main Justice and the Southern District of New York, that had not also been produced to our office.

## II. ARGUMENT AND AUTHORITY

### A. A *Brady* Order is unnecessary because the government has repeatedly demonstrated that it understands and complies with its *Brady* obligations.

If the Court were to issue the *Brady* order requested by the defense, that order would have no practical effect because the government is already complying with its obligations under Ninth Circuit law and Department of Justice policy. *See* Justice Manual § 9-5.001(B)(1). The irony of Thompson's motion is that, out of an abundance of caution consistent with DOJ standards, our office obtained and produced documents from Main

---

[1] The government considered an email exchange to be "non-duplicative" even if it was merely a one-line reply that previously had not been produced to a five-page email string that previously had been produced. As a result, the actual amount of new information produced was substantially less than 300 pages.

[2] Defense claims in their motion that "Defense counsel inquired with Seattle-based prosecutors whether the PowerPoint presentation was made to Main Justice or the Southern District of New York, but the government has not answered that question." Def.'s Mot. at 5. That is not correct. The government sent an email responding to the inquiry, attached as Exhibit 2, that noted (1) defense counsel had already sent an email to the government acknowledging that the presentation was made to Main Justice, (2) the government previously had responded confirming that fact, and (3) that was in fact the case – the presentation was made to Main Justice. Exhibit 2.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Justice without analyzing the materiality of the documents and without analyzing whether Main Justice is part of our prosecution team. We do not agree that Main Justice is a member of our prosecution team, nor do we agree that the Main Justice documents are material to guilt or punishment, or favorable to the defense, as explained in Section C, below. But, rather than asserting those positions, as soon as we became aware of it, our office simply gathered the material held by Main Justice and produced it.

To be clear, this is not a situation in which the government is in possession of potential discovery but withholding it on the basis of privilege or materiality. Rather, as the discovery production shows, the government gathered discovery that we did not think was material or exculpatory and produced it anyway.

This also is not a situation in which there is any reason to believe that there is any other discoverable material within the possession of any other entity that could be considered part of the prosecution team.[3] We have confirmed with Main Justice and the Southern District of New York that they did not further investigate or gather additional materials beyond the documents we have produced, or the defense has already received. And we confirmed with Capital One that it had not produced any additional information to any other component of the Department of Justice, including the FBI.

For both of these reasons this is not a case in which there is any basis for special concern that the government is not complying with its *Brady* obligations, or for the Court to take any action beyond that which it normally would take in a criminal case.

//

//

[3] The defense also alludes in its motion to materials gathered by the Office of the Comptroller of the Currency (OCC). Def.'s Mot. at 4. That office gathered massive amounts of information from Capital One in the course of its regulatory investigation. After the defense asked the government to produce these, the government explained, in four letters—sent in 2020, and which are attached—that the OCC is not part of the prosecution team, and the government has no obligation to assemble and produce materials in the possession of the OCC. *See* Exhibits 3-6. To the extent that the defense is attempting to challenge this and obtain these materials nearly a year-and-a-half later, and more than three months after the motions deadline in this case, that claim is untimely and has been waived.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**B. If the Court issues a *Brady* Order, it should issue the Due Process Protection Act Order that is routinely entered in this District.**

In October 2020, Congress enacted the Due Process Protections Act (DPPA), which amended Federal Rule of Criminal Procedure 5 to require a judge to issue an order "that confirms the disclosure obligation of the prosecutor under *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny" at the beginning of every case, and requires each judicial council to promulgate a model order for the district courts within its judicial circuit. Pub. Law No. 116-182 (Oct. 21, 2020). The legislative history of the DPPA confirms that the act was intended to "reinforce the government's already existing constitutional obligation to disclose exculpatory evidence."[4] 166 Cong. Rec. H4582-01.

After careful consultation with the United States Attorney's Office and the Office of the Federal Public Defender, the Western District of Washington developed and implemented a model *Brady* order that is now given in all new cases, at a defendant's initial appearance. It states:

> Pursuant to the Due Process Protection Act, counsel for the government is reminded of his/her obligations pursuant to *Brady v. Maryland* and its progeny to disclose exculpatory material and information, as required by applicable statute and case law. The failure to do so in a timely manner may result in dismissal of the indictment or information, dismissal of individual charges, exclusion of government evidence or witnesses, or any other remedy that is just under the circumstances.

*See, e.g., United States v. Shuemake*, CR21-194 RAJ (Dkt. 8); *United States v. Faglier*, CR21-196 JCC (Dkt. 18); *United States v. Navarro*, CR21-210 RSM (Dkt. 15); *United States v. Bock*, CR22-024 JCC (Dkt. 11); *United States v. Moore*, CR22-013 LK (Dkt. 10); *United States v. Guyton*, CR22-030 RSM (Dkt. 9).

[4] This intent is consistent with a Standard Order in the Eastern District of Washington, highlighted by the defense in a Notice of Supplemental Authority (Dkt. 217). That order states: "Nothing in this Disclosure Order enlarges or diminishes the Government's obligation to disclose information and evidence to a defendant under *Brady*, as interpreted and applied under Supreme Court and Ninth Circuit precedent." *Id.* at 4-5.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Because Thompson's case was filed before the DPPA was enacted, a DPPA order has not been entered. The government does not object to the Court entering a DPPA order in this case that is consistent with the model language routinely used in this District. Any additional language—like that contained in Thompson's proposed order—is unnecessary because there is no actual dispute regarding the scope of the government's *Brady* obligations and it would represent a substantial departure from the carefully negotiated model language used in this District.

The Justice Manual § 9-5.001 recognizes, consistent with *United States v. Bagley*, 475 U.S. 667, 676 (1985), and *Kyles v. Whitley*, 514 U.S. 419, 439 (1995), that the government's *Brady* obligations only extend to material exculpatory evidence. However, the Justice Manual requires federal prosecutors to "take a broad view of materiality and err on the side of disclosing exculpatory and impeaching evidence." *Id.* "While ordinarily, evidence that would not be admissible at trial need not be disclosed, this policy encourages prosecutors to err on the side of disclosure if admissibility is a close question." *Id.* The government's discovery productions in this case are evidence that the government understands, and is complying with, its obligations.[5]

**C. The government disagrees that the Main Justice documents are material or exculpatory *but has produced them anyway.***

The government has not withheld evidence based on our analysis of materiality or favorability and the defense has no basis to claim that we have. Main Justice subpoenaed documents from Capital One regarding the March 2019 note without this office's knowledge.[6] Because our office did not coordinate activities with Main Justice, and

[5] There will of course be additional discovery in the case. The government is continuing to generate discovery as it conducts additional investigation and interviews. The government will produce such discovery on a rolling basis, as interviews occur, even though pretrial production is not required under the *Jencks* Act, 18 U.S.C. § 3500 or Federal Rule of Criminal Procedure 26.2.

[6] As the defense notes in its pleadings, Thompson's "white hat hacker" defense was not apparent to the government until October 2021, at the absolute earliest. From the government's perspective, this defense was not apparent until the defense filed its pretrial motions in early December 2021. Regardless, had the government learned earlier that



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

because our investigative agency, the FBI, was not involved, we did not know that the Main Justice documents existed. Had we been aware of these documents earlier, we would have produced them earlier. We have now confirmed with Capital One, Main Justice, and the Southern District of New York that the defense has received all the materials Capital One provided to those entities. Main Justice and the Southern District of New York further confirmed they do not have any investigative materials beyond what they received from Capital One.

Moreover, far from being exculpatory, the government believes that the May 2019 note, and Capital One's investigation of it, are irrelevant to the charges in the Second Superseding Indictment. Thompson copied data from Capital One's servers on March 22-23, 2019—two months before an unknown person passed a note to Amazon that may or may not be related to Thompson. No one, not even Amazon, knows who passed the note. Capital One was not able to understand the note, identify the vulnerability, fix the vulnerability, or contact the person who passed the note for further information. The note referred to an "open socks proxy," and the vulnerability that enabled Thompson's intrusion was not an "open socks proxy." Even if Capital One had understood the vulnerability in the note and fixed it, Thompson had already stolen its data two months earlier.

In fact, Capital One's investigation of the May 2019 note is actually *inculpatory*. The defense has repeatedly argued—as recently as two days ago—that Thompson's conduct was not criminal because Capital One "chose" to misconfigure its Web Application Firewall in a way that authorized public access to its security credentials. Capital One's obvious concern about the accessibility of its private, internal security credentials and its efforts to find and eliminate external access to those credentials are

---

Main Justice gathered documents related to Thompson's intrusion, we would have produced them, even without knowing the defense's "white hat hacker" theory, in accordance with DOJ policy and practice.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

further evidence that Thompson's earlier intrusion and use of Capital One's security credentials was unauthorized.

Finally, the defense has mischaracterized the substance of the Main Justice documents. Of the roughly 300 pages that were produced by our office, 135 pages were Capital One's 2020 proxy statement and annual report to shareholders, which are publicly available. Many of the remaining pages were copies of the same email strings that had been provided to the defense, in one form or another, at least 20 times. At most, there were approximately 50 pages of new material relating directly to the technical aspects of Thompson's intrusion. And that material was cumulative of, and consistent with, other material about the technical aspects of the breach that the defense received in July 2021, such as an 18-page Intrusion Investigation Report summarizing Mandiant's technical analysis of Thompson's intrusion, and a "PONG Event Summary" summarizing Capital One's technical analysis and recommendations after investigating the May 2019 note.

It also is disingenuous for the defense to suggest that the Main Justice materials informed them, for the first time, that Capital One did not believe that Thompson disseminated its data or used it for fraudulent purposes. Def.'s Mtn., p. 3 (Dkt. 207). The defense has repeatedly highlighted similar statements from Capital One in its pleadings, beginning on August 20, 2019. *See* Def.'s Resp. to Gov't Mem. In Support of Mtn. for Detention, p. 11 (Dkt. 19).

//

//

//



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## III. CONCLUSION

For the foregoing reasons, the Court should deny the defense motion, or, alternatively, enter an order consistent with the Due Process Protection Act.

DATED this 17th day of March, 2022.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

*/s Andrew C. Friedman*
*/s Jessica M. Manca*
*/s Tania M. Culbertson*
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7970
Fax: (206) 553-0882
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov
Tania.Culbertson@usdoj.gov